IPSWITCH

WhatsUp Event Analyst
v10.x
Database and Reporting
Optimization Guide

WhatsUp Event Analyst Database and Reporting Optimization Guide

WhatsUp Event Analyst Database and Reporting Optimization Guide

In This Guide

Indexing Considerations

By default, when WhatsUp Event Archiver, WhatsUp Event Alarm, or WhatsUp Event Analyst create tables in an ODBC database such as Microsoft SQL Server or Oracle, they do not add indexes to the table. Small organizations whose servers produce few log records may not need to index their event log tables. However, organizations that send large volumes of records to a database server on a regular basis (e.g. via WhatsUp Event Archiver or WhatsUp Event Alarm) should take advantage of table field indexing to speed data retrieval during filtering and reporting inside WhatsUp Event Analyst.

While indexing is excellent for speeding up data retrieval during filtering and reporting, it does increase overhead (including CPU, memory, and storage space) on the database server when new records are imported into indexed tables, as the indexes must be updated at that time. Therefore, before applying indexes to your event log tables, make sure WhatsUp Event Archiver's log collection is scheduled for off-peak times, and make sure that your database server has the horsepower and storage to handle index maintenance when new records flow into these tables.

Using WhatsUp Event Analyst to Create Indexes

When setting up links to Microsoft Access and Microsoft SQL Server database tables in WhatsUp Event Analyst's Database Table Links Manager dialog (**File** menu > **Manage Database Table Links**), you can also elect to index the table at that time. When adding or editing a new database source, open your database, select a table, and click the **Index Table** button. The indexes applied to your table are the same ones discussed in the next section. If your table is already quite large, it may take many minutes, or in some cases, several hours, to apply the index. It is best to index tables while they are still small.

Versions 4 and later of WhatsUp Event Analyst feature automatic detection and configuration of WhatsUp Event Archiver database tables in the Database Table Links Manager dialog. If you elect to have WhatsUp Event Analyst auto-configure the WhatsUp Event Archiver tables for use with WhatsUp Event Analyst when prompted, default indexes are applied to the tables during this process. No further indexing is required, unless you wish to target other fields with custom filters. Consult with your database administrator on how to apply additional indexes to your database tables beyond the default indexes mentioned below.

Default Indexes Applied To Database Tables By WhatsUp Event Analyst

DateAndTime Field (Clustered Index)

EventID Field (Non-Clustered Index)

LogType Field (Non-Clustered Index)

For best performance with WhatsUp Event Analyst's default indexes, create filters that target date/time ranges and/or individual or multiple Event IDs.

Scripting Index Creation in Microsoft SQL Server

While WhatsUp Event Analyst can index tables on demand when setting up database table links (e.g. by using the "Index Table" button), some administrators may want to run scripts directly on the database server to index many different tables at once.

The following script adds three indexes that offer significant performance enhancements for the majority of predefined filters and reports that come with WhatsUp Event Analyst. If you plan to filter on log record fields other than the ones targeted by WhatsUp Event Analyst's default indexes, consult with your database administrator on how to create additional indexes that target those fields.

This script is designed for Microsoft SQL Server. Oracle database users need to create their own similar indexes on the DateAndTime, RecordNum, and EventID fields.

To use the following SQL Script to create indexes on your WhatsUp Event Archiver or WhatsUp Event Alarm tables, copy the portion of the script below these comments into the Microsoft SQL Server Query Analyzer. Before executing the script, do an **Edit > Replace** for all occurrences of "SecurityLogs", replacing them with the name of the table you wish to index. Then, after the table names are correct, execute the script to add the indexes to your table.

*/

BEGIN TRANSACTION

SET QUOTED_IDENTIFIER ON

GO

SET TRANSACTION ISOLATION LEVEL SERIALIZABLE

GO

COMMIT

BEGIN TRANSACTION

CREATE CLUSTERED INDEX IX_SecurityLogs_DateAndTime ON SecurityLogs

(

DateAndTime

) ON [PRIMARY]

GO

CREATE NONCLUSTERED INDEX IX_SecurityLogs_EventID ON SecurityLogs

(

EventID

) ON [PRIMARY]

GO

ALTER TABLE SecurityLogs ADD CONSTRAINT

PK_SecurityLogs PRIMARY KEY NONCLUSTERED

(

RecordNum

) ON [PRIMARY]

GO

COMMIT

Speeding Up Reporting in WhatsUp Event Analyst

Reporting against database tables in WhatsUp Event Analyst is the quickest method of producing reports. Unlike some flat files (such as EVT files or TXT files), database tables can be indexed, which provides very quick retrieval of only the records most significant to a report or filter. If you want to routinely collect your servers' and workstations' event logs into database tables on a scheduled or near real-time basis, evaluate Ipswitch's other event log management tiles, WhatsUp Event Archiver and WhatsUp Event Alarm.

After you have applied indexes to your event log database tables, use WhatsUp Event Analyst's Advanced Filters and Quick Date Filters to your advantage. The easiest way to reduce the size of data being reported against is to apply a Quick Date Filter to a database table link before opening it. Because the DateAndTime field is a field that WhatsUp Event Analyst indexes by default, limiting data by a date range is a wonderful way to speed up report creation. When opening up a table or view from an ODBC data source inside WhatsUp Event Analyst, limit the records returned to you by clicking the **Enable Date Filter** button, and specifying a date range of a few days over which to return records. By filtering records in this manner, WhatsUp Event Analyst has a much smaller result set to report across.

Advanced filters can also reduce the volume of data in a variety of ways. No matter what other fields you are searching for (e.g. certain Users, certain Event IDs, etc), make sure to enable Date/Time filtering and select a Relative Range to only return records that occurred in the past X number of days. After you have defined an advanced filter in this manner (click the **Edit** menu > **Define Advanced Filters** to do this), remember to select it when opening up an ODBC database source by clicking the **Filters** button before clicking the **Show Results In Window** or **Build Report** buttons.

When scheduling a report using WhatsUp Event Analyst's Report Scheduler, use the **Only report over the last __ days** option to reduce the number of records WhatsUp Event Analyst must process when building a report.